

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/9/2009

SUBJECT:

Multiple Vulnerabilities in Adobe Products Could Allow Remote Code Execution

OVERVIEW:

Seven vulnerabilities have been discovered in Adobe Flash Player and Adobe AIR. Adobe Flash Player is a widely distributed multimedia and application player for Microsoft Windows, Mozilla, and Apple systems. It is used to enhance the user experience when visiting web pages or reading email messages. Adobe AIR allows users to develop web applications that will work outside of a web browser. These vulnerabilities can be exploited if a user visits a malicious website or opens an email attachment containing Flash media designed to exploit these vulnerabilities.

Successful exploitation of six of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Failed exploitation could result in denial-of-service conditions. The remaining vulnerability will allow access to potentially sensitive information (e.g., username, passwords, credit card information).

SYSTEMS AFFECTED:

Adobe Flash Player 10.0.32.18 and earlier
Adobe AIR 1.5.2.8900 and earlier

RISK:

Government:

Large and medium government entities: High
Small government entities: High

Businesses:

Large and medium business entities: High
Small business entities: High

Home users: High

DESCRIPTION:

Seven security vulnerabilities have been identified in Adobe Flash Player and Adobe AIR. These vulnerabilities can be exploited if a user visits a malicious website or opens an email attachment containing a Flash media file designed to trigger these issues.

One vulnerability is caused by memory corruption which causes a JPEG Parsing error.

One vulnerability is caused by an unspecified Data Injection Vulnerability.

Three vulnerabilities are caused by unspecified Memory Corruption errors.

One vulnerability is caused by an Integer Overflow error.

One vulnerability allows for the unauthorized disclosure of information.

Successful exploitation of six of these vulnerabilities could allow for the execution arbitrary code on the affected system. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Failed exploitation could result in denial-of-service conditions. The remaining vulnerability will allow access to potentially sensitive information (e.g., username, passwords, credit card information).

Adobe has released upgraded versions of Adobe Flash Player, version 10.0.42.34, and Adobe AIR, version 1.5.3.9120, that address all of the reported vulnerabilities.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the recommended software version based on Adobe's security advisory.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments from unknown or un-trusted sources.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/37199>

Secunia:

<http://secunia.com/advisories/37584/>

Vupen:

<http://www.vupen.com/english/advisories/2009/3456>

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb09-19.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4820>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3794>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3796>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3797>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3798>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3799>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3800>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3951>